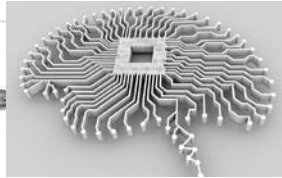


Extending Blockchains with AI for Risk Management



Raj Jain

Barbara J. and Jerome R. Cox, Jr. Professor
Washington University in St. Louis

jain@wustl.edu

Keynote at the International Conference on Intelligent Computing and Security: A Paradigm Shift (IICS2021), GL Bajaj Inst. Of Technology and Management, Greater Noida, India, December 17, 2021

Slides and Video Recording of this talk are at:

http://www.cse.wustl.edu/~jain/talks/psc_iics.htm



1. Strength of blockchains
2. Weaknesses of the blockchains
3. **Extending blockchains**: Converting data to knowledge
4. Applications of **Knowledge Chains**
5. **Issues** in applying AI to IoT Security

What is a Blockchain?



1. Satoshi Nakamoto invented Bitcoin
2. He used blockchains to make it decentralized
3. Since then blockchains have found numerous other applications
4. Blockchains allow two complete strangers to enter into a smart contract without a trusted third party.
5. This talk is about blockchains, not about Bitcoin.



Example of a Contract: Wedding



Example of a Contract: Wedding



- ❑ Centralized registry
- ❑ Single point of failure
- ❑ Easier to hack



- ❑ Decentralized
- ❑ No single point of failure
⇒ Fault Tolerant, No Monopoly
- ❑ Very difficult to hack

Examples of Centralized Systems

- ❑ **Banks:** Allow money transfer between two accounts
- ❑ **City Records:** Wedding registers, Property ownership
- ❑ **Networks:** Certificate Authorities, DNS

❑ In all cases:

- There is a central third party to be trusted
- Central party maintains a large database ⇒ Attracts Hackers
- Central party may be hacked ⇒ Affects millions
- Central party is a single point of failure.
Can malfunction or be bribed



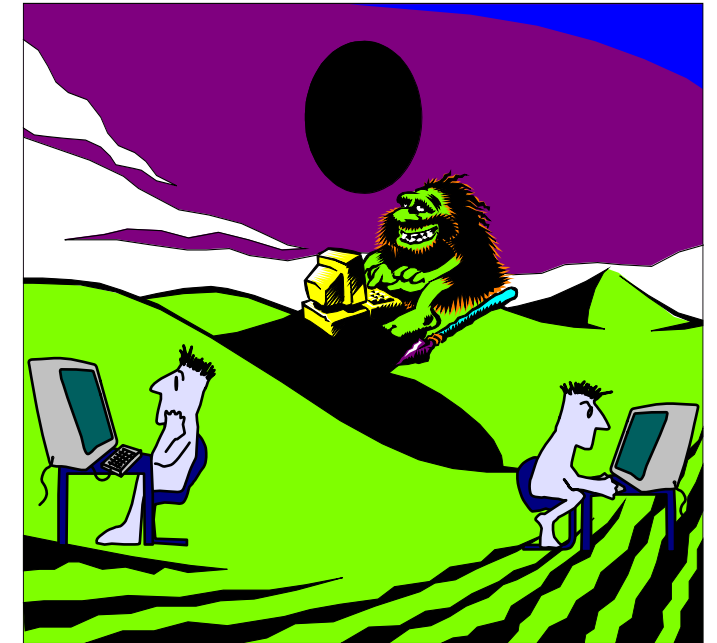
Trend: Decentralized \Rightarrow Centralized \Rightarrow Decentralized



Decentralized



Industrialization \Rightarrow Centralized



COVID \Rightarrow Decentralized

Time is a cycle: Decentralized vs. Centralized debate

Key Strengths of Blockchains

1. **Distributed:** No single point of failure
2. **Decentralized Consensus:** Transactions valid only if agreed by majority
3. **Trustless:** Transacting or processing parties do not need to trust
4. **Cryptographic Security:** Elliptic Curve Cryptography
5. **Non-Repudiation Guarantee:** All transactions are signed

Can the Blockchains be Enhanced?

Limitation 1: Only facts are recorded

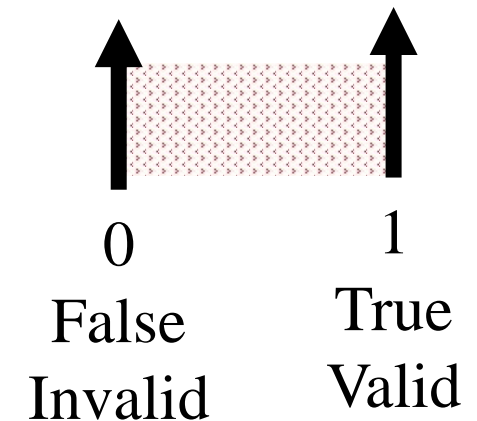
- ❑ Alice is married to Bob
- ❑ Alice gave 20 coins to Bob
- ❑ Alice signed a contract with Bob to pay 10 coins for 1 kg of xx.

Limitation 2: Binary Validity

- ❑ All transactions recorded on the blocks that are committed are valid
- ❑ Those not on the committed blocks and old are invalid
- ❑ So the recording is binary: only 0 or 1.

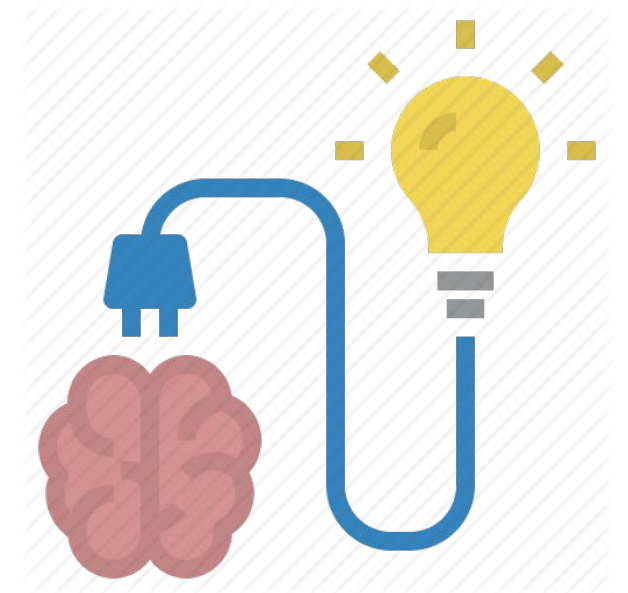
Limitation 3: Deterministic Events only

- ❑ Can not record that I am only 90% sure that Alice gave 20 coins to Bob.



Ideas to Enhance Blockchains

- ❑ Blockchain is just a distributed **data storage** of valid transactions
- ❑ All transactions are *deterministic*
- ❑ What's Wrong?
 - Need to convert data to **knowledge**
 - We are in big data and **machine learning** age
 - Real life is **probabilistic**
 - Most to the decisions we make are probabilistic
⇒ All decisions have some **risk**



Decisions with Risk

- ❑ Sell insurance
- ❑ Buy insurance
- ❑ Sell a stock
- ❑ Buy a stock
- ❑ Download a software application on your computer
- ❑ Update your computer
- ❑ Marry someone



Risk Propels Progress

- ❑ Banks take money from risk-averse savers and give them interest
- ❑ Banks invest the money in corporations
⇒ Takes the country forward
- ❑ Venture capitalists take risk by investing in half-cooked ideas
- ❑ Startups take risk by working in uncharted territories

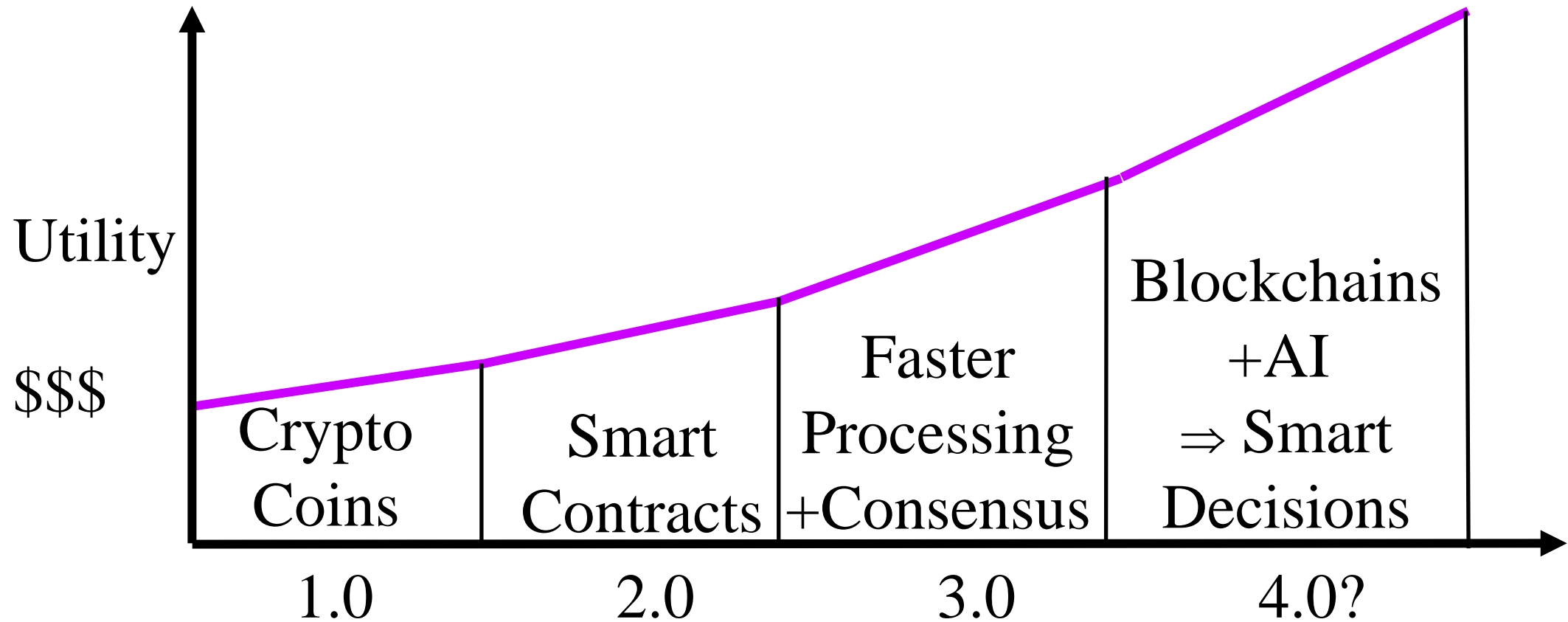


Our Goal

- ❑ Moving the chain from deterministic to **probabilistic**
- ❑ Moving the chain from storage to **computation**
- ❑ Moving the chain from data to **knowledge**
- ❑ Moving the chain from information to **decision making**

- ❑ Google is moving from “Search” to “Suggest” using AI
- ❑ A blockchain that provides knowledge
 - A **knowledge chain** would be more useful

Blockchain Generations



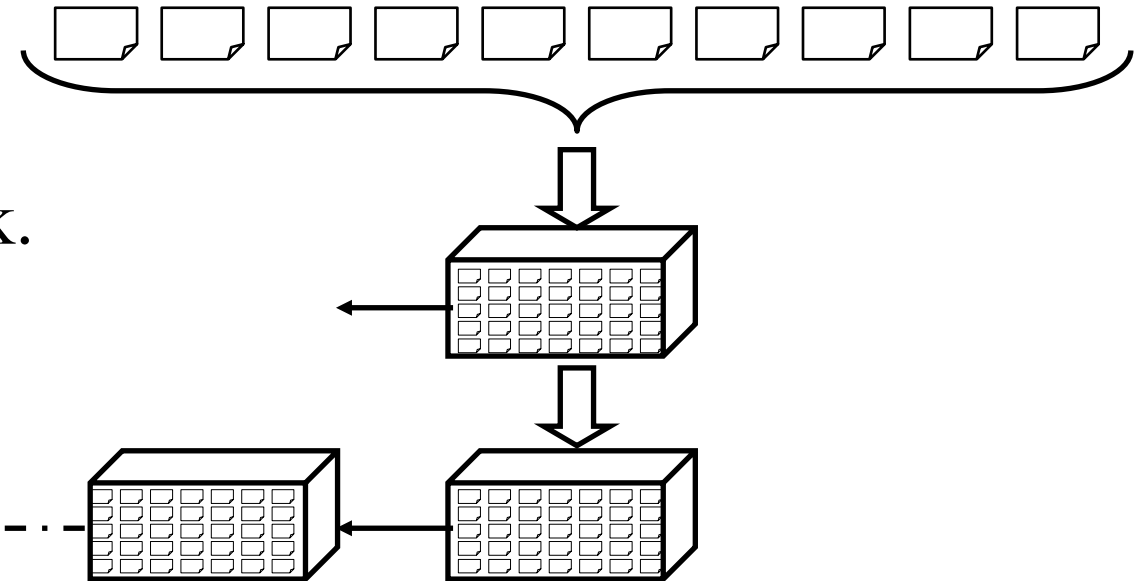
Blockchain Process

1. **Users** broadcast signed transactions or smart contracts

2. **Mining nodes** validate transactions and create blocks. Point to previous block.

3. **Blockchain nodes** validate blocks and construct a chain

□ There are many users, many mining nodes, and many blockchain nodes. More nodes \Rightarrow Better. Less \Rightarrow Blockchain not required/useful.



Knowledge Chain / Probabilistic Blockchain

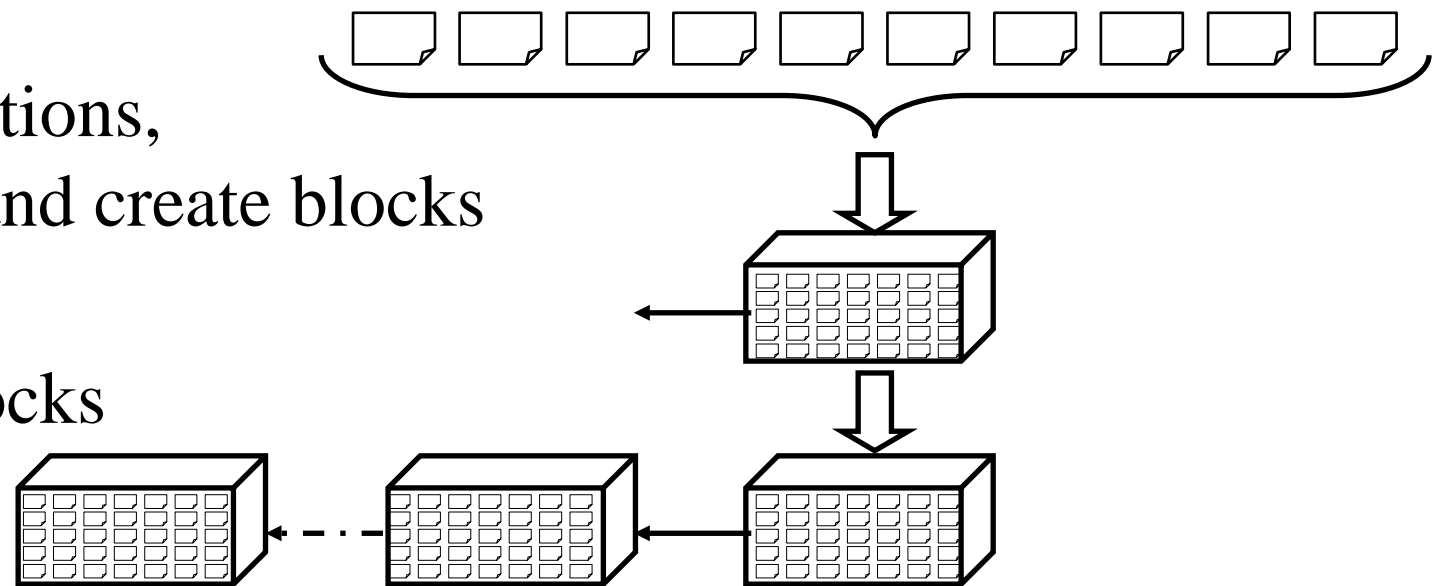
1. **Agents** broadcast transactions,
Transactions = Opinions/decisions

2. **Mining nodes** validate transactions,
create a knowledge summary and create blocks

3. **Blockchain nodes** validate blocks
and construct a chain

□ Two types of users:

- **Agent nodes** provide their probabilistic opinions/decisions
- **Management nodes** that inquire the blockchain and use it for group decisions



Knowledge Chain Example

- **Issue:** Whether Cisco stock will go up tomorrow?
- i^{th} Agent says that the probability that it will go up is p_i
- Summary of all opinions related to this issue is:

$$P[\text{Stock will rise}] = G(\{p_1, p_2, \dots, p_n\})$$

Here, G = Machine Learning Algorithm = Summarizing function

Ref: T. Salman, R. Jain, and L. Gupta, "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, Nov. 8-10, 2018, 9 pp.,

http://www.cse.wustl.edu/~jain/papers/abc_uem.htm

Washington University in St. Louis

http://www.cse.wustl.edu/~jain/talks/abc_iics.htm

©2021 Raj Jain

Generalizing the Summary Function

- ❑ Summary can be any other reasonable function of individual decisions:
 - 90-percentile
 - Median
 - Mode
 - 2nd Moment
- ❑ Summary can be a vector: { 1st moment, 2nd moment, ..., n^{th} moment }
- ❑ Summary can be the result of any **statistical** algorithm
- ❑ Summary can be the result of a **data mining** algorithm
- ❑ Summary can be the result of a **machine learning algorithm**

Empirical Validation

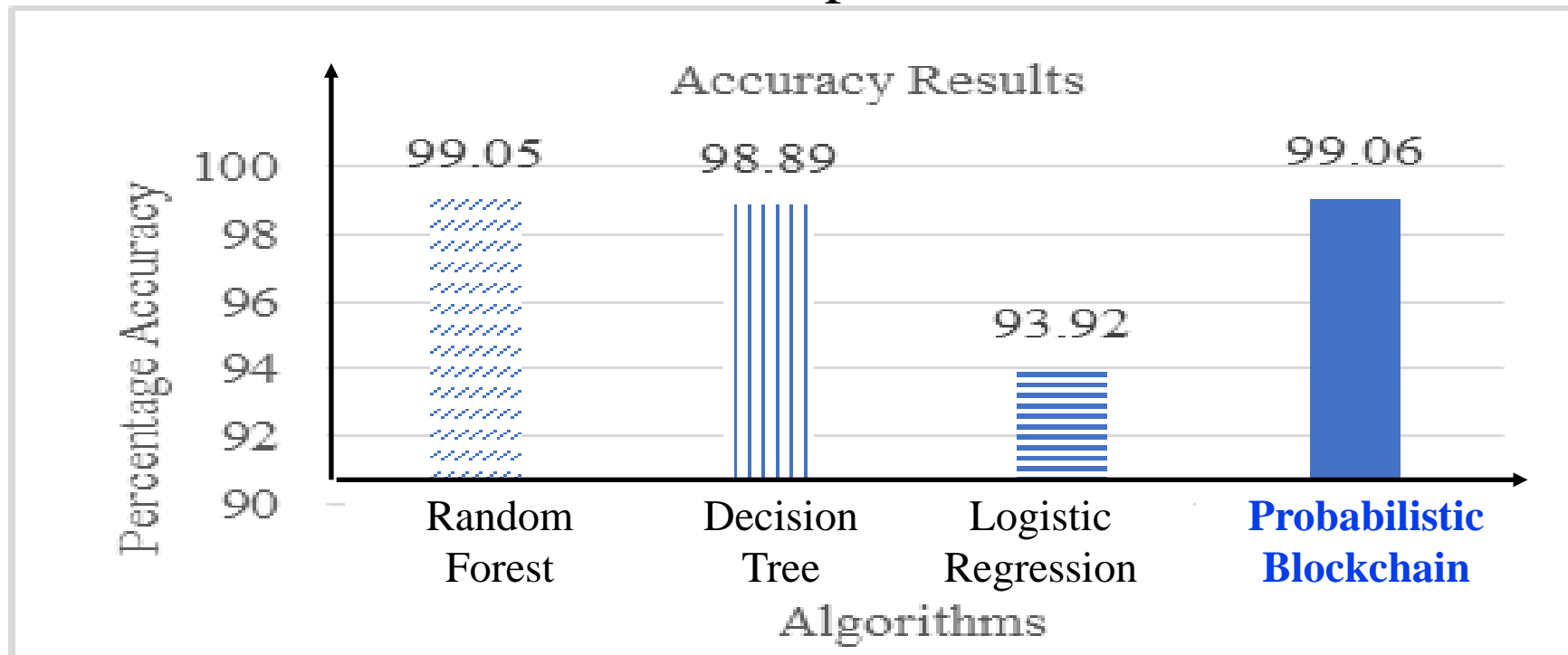
- ❑ Issue: Whether a network traffic pattern represents intrusion
- ❑ 1000 Agents* using different machine learning algorithms give their decisions: Yes or No
- ❑ Mining nodes summarize these decisions using the majority function

$$P = \frac{1}{n} \sum p_i$$

*In our simulation, agent modules randomly pick one of the 3 algorithms:
Random Forest, Decision Tree, Logistic Regression

Results

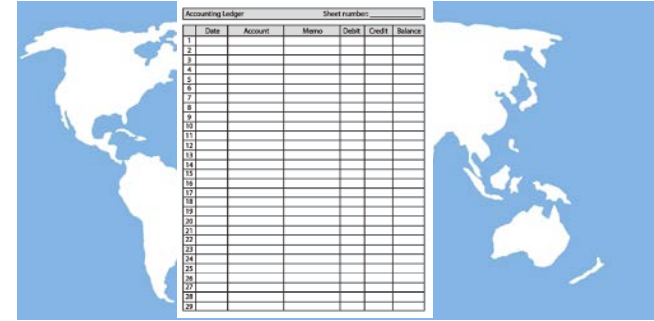
$$\text{Accuracy} = \frac{\text{Correct Predictions}}{\text{Overall Samples}} \times 100\%$$



Distributed decision making is better than any individual decision

Blockchain 4.0: Database to Knowledge Base

- ❑ Blockchain = Distributed ledger/database
- ❑ Probabilistic blockchain = Knowledge + database
- ❑ **Database:** Who bought, who sold, what quantity, what price, what time
- ❑ **Knowledge:**
 - Where the market is going?
 - Whether we should buy, sell, or hold?
 - Is this a fake news? Spam? Fraud?



The image shows a world map with a central accounting ledger table. The table has columns for Date, Account, Memo, Debit, Credit, and Balance. The rows are numbered 1 through 29.

Accounting Ledger						Sheet number:	
1	Date	Account	Memo	Debit	Credit	Balance	
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							

Knowledge Chain

- ❑ Customer query to blockchain network:
How is the Cisco stock doing today?
- ❑ Blockchain to Customer: With 60% confidence, the probability of stock rising is 90%, ...
- ❑ Ideal for **large** distributed systems with **no national boundaries**, no exchange limitations, no brokers in between
- ❑ **Crowd-sourced knowledge**, crowd-sourced decisions

Application Examples

1. Spam from Email/IP Addresses/Cloud providers/source/public IP
2. Intrusions/attacks from IP Addresses. Anonymously share attack information.
3. Gray domains: Share gray list among agents.
4. Reliability/Issues with recent software updates
5. Error/reliability statistics of network/IoT devices
6. Virus in software

Issues to Resolve

1. **Summary functions**
2. **Overhead of consensus mechanisms:** Proof of Work, Proof of Stake, ...
3. **Reputation of Experts and Bad Actors:**
 - Some agents are better than others
 - Group decisions should give more weight to them
 - How to incentivize better agents
 - How to penalize bad actors

Reputation Management

□ Requirements:

- Dynamic: Old mistakes count less than recent mistakes
- Configurable Parameters: E.g., penalty/reward.
Different applications have different risk levels
- Proportional Trust: Good performers trusted 100%
while bad performers trusted 0%
- ...

□ Solution: Rated Proportional Multi-Configurable Exponentially Weighted Average (RPMC-EWA)

Ref: T. Salman, R. Jain, and L. Gupta, "A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains," IEEE 1st International Workshop on Advances in Artificial Intelligence for Blockchain (AICChain2019), held in conjunction with the 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019.

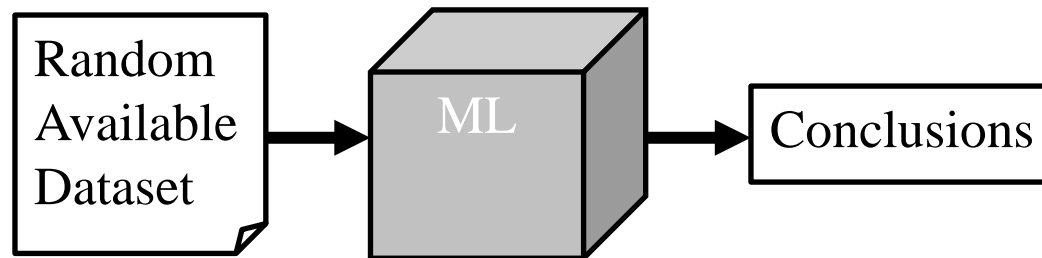
Washington University in St. Louis

http://www.cse.wustl.edu/~jain/talks/pbc_iics.htm

©2021 Raj Jain

Machine Learning Challenges

- ❑ Machine learning is currently a black box
- ❑ ML algorithms are developed/used without domain expertise
- ❑ Data cleanliness, labeling, feature extractions, all require domain knowledge, e.g., What is the distance between Port 80, Port 81, and Port 8080?
- ❑ Synthetic data is used \Rightarrow Garbage-In, Garbage-Out
- ❑ Results are stated without model validation.



Ref: Lav Gupta, Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, "Fault And Performance Management In Multi-Cloud Virtual Network Services Using AI: A Tutorial And A Case Study," Computer Networks, Pre-Proof published on 14 Oct 2019,

http://www.cse.wustl.edu/~jain/papers/fp_comst.htm

AI for Security Issue 1: Imbalance

- ❑ AI started with image analysis but needs to be extended for security
- ❑ Security data is very different from image data
 - Most security datasets are not representative of real world.
 - In most papers, 10-15% of the packets are attack packets
- ❑ In real-world, 1 in a billion packets is an attack packet
 - Mis-classify the attack packet \Rightarrow 99.9999% accuracy
 - Current metrics and methods not suitable for highly imbalanced
- ❑ **Data imbalance** is a key issue in AI for security



1% attack

Ref: Maede Zolanvari, Marcio A. Teixeira, Raj Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp.,

http://www.cse.wustl.edu/~jain/papers/imb_isi.htm

AI for Security Issue 2: Wrong Metrics

- ❑ In Image analysis:
Cost of predicting 0 when it is 1 = Cost of predicting 1 when it is 0
⇒ Cost of errors is symmetric
- ❑ In Cyber Security:
 - Cost of missing an attack = $10^6 \times$ Cost of false attack prediction
- ❑ Accuracy is not a good metric for security
- ❑ Need new metric to find the best algorithm
⇒ Use Safety Score

Ref: Tara Salman, Ali Ghubaish, Devrim Unal, Raj Jain, "Safety Score as an Evaluation Metric for Machine Learning Models of Security Applications," IEEE Networking Letters, Vol. 2, Issue 4, December 2020, pp. 207-211, <http://www.cse.wustl.edu/~jain/papers/safety.htm>

Trustable AI

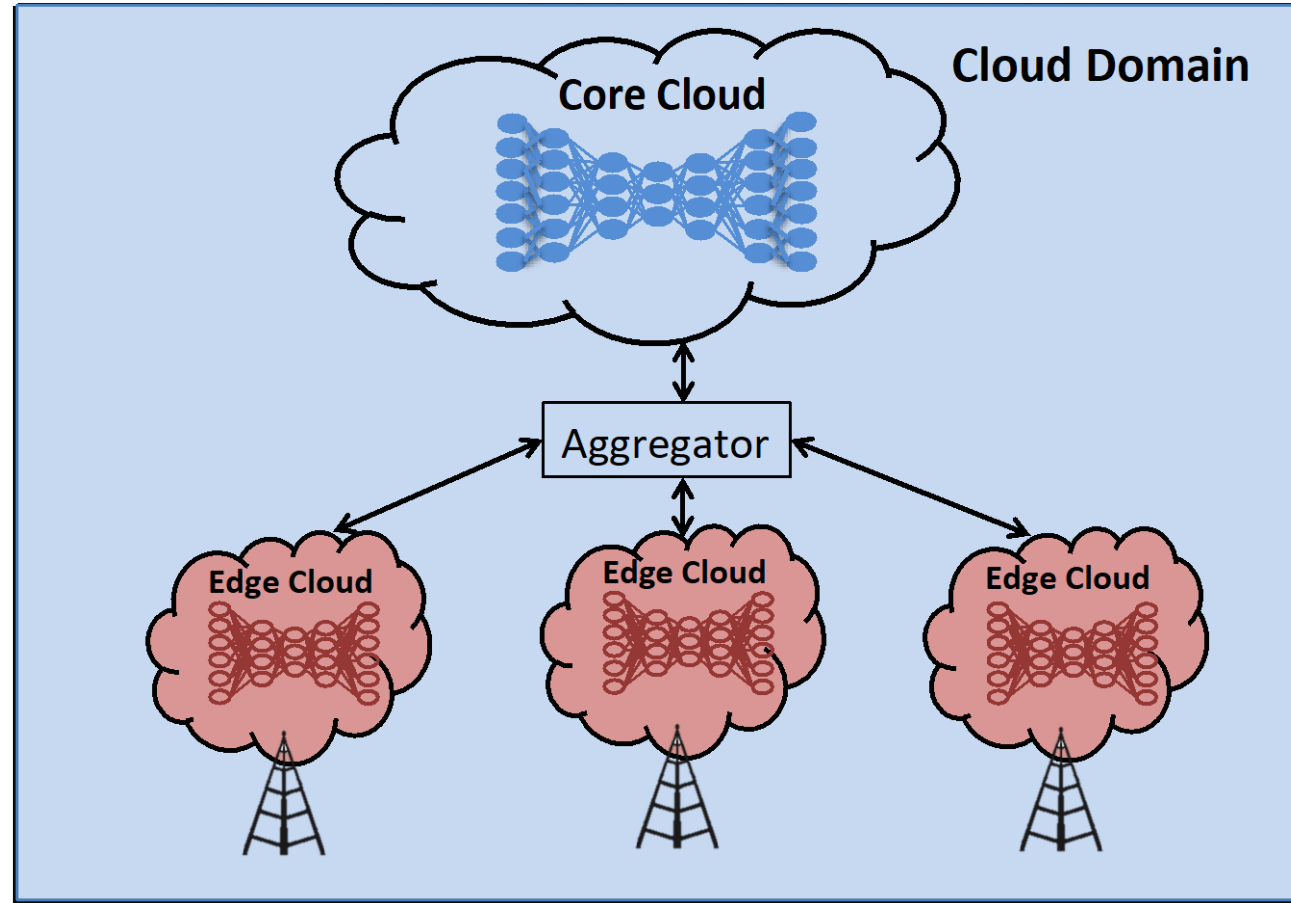
- ❑ Would you trust AI to diagnose your disease?
- ❑ Would you trust AI to National Cybersecurity?
- ❑ No, because you have no idea of why the results are what they are
⇒ Can't discover bugs in ML model implementations
- ❑ Trustable AI = Explainable AI
⇒ AI that can be understood by humans



*Machine Learning is what only machines can do,
but human cannot do and cannot explain*

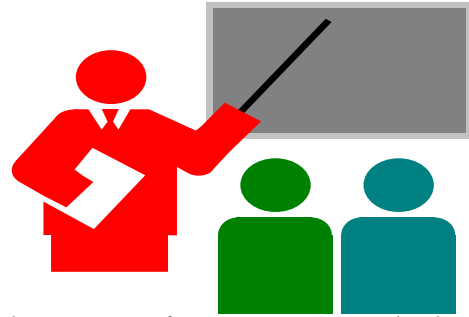
Ref: Maede Zolanvari, Zebo Yang, Khaled Khan, Raj Jain, and Nader Meskin, "TRUST XAI: A Novel Model for Explainable AI with An Example Using IIoT Security," IEEE IoT Journal, preliminary acceptance, September 2021.

Distributed/Federated AI



Ref: Lav Gupta, Tara Salman, Ali Ghubaish, Devrim Unal, Abdulla Khalid Al-Ali, Raj Jain, "Cybersecurity of Multi-Cloud Healthcare Systems: A Hierarchical Deep Learning Approach" Under Review.

Summary



1. Blockchains provide an immutable, secure, distributed database
2. Three generations: Cryptocurrency, Smart contract, faster performance.
All three generations are deterministic and **only provide storage**
3. The next generation needs to **connect computation and AI** to make knowledge/decisions in addition to data storage
4. Consensus can be the probabilistic result of any statistical algorithm, data mining, or machine learning \Rightarrow **Knowledge Chain**
5. Need to use different metrics for Security.

Related Papers

- ❑ Tara Salman, Raj Jain, and Lav Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/psc_uem.htm
- ❑ Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "**Security Services Using Blockchains: A State of the Art Survey**" IEEE Communications Surveys and Tutorials, Accepted September 2018, 28 pp., <http://www.cse.wustl.edu/~jain/papers/bcs.htm>
- ❑ T. Salman, R. Jain, and L. Gupta, "**A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains**," 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019, <http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm>

Related Papers (Cont)

- ❑ Tara Salman, Ali Ghubaish, Devrim Unal, Raj Jain, "**Safety Score as an Evaluation Metric for Machine Learning Models of Security Applications**," IEEE Networking Letters, Vol. 2, Issue 4, December 2020, pp. 207-211, <http://www.cse.wustl.edu/~jain/papers/safety.htm>
- ❑ Maede Zolanvari, Marcio A. Teixeira, Lav Gupta, Khaled Khan, Raj Jain, "**Machine Learning Based Network Vulnerability Analysis of Industrial Internet of Things**," IEEE Internet of Things Journal, Vol. 6, Issue 4, Aug 2019, <http://www.cse.wustl.edu/~jain/papers/vulnerab.htm>
- ❑ Marcio Andrey Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, and Mohammed Samaka, "**SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach**," Future Internet 2018, 10(8), 76, http://www.cse.wustl.edu/~jain/papers/ics_ml.htm
- ❑ Lav Gupta, Tara Salman, Ria Das, Aiman Erbad, Raj Jain, Mohammed Samaka, "**HYPER-VINES: A HYbrid Learning Fault and Performance Issues ERadicator for Virtual Network Services over Multi-cloud**," International Workshop on Computing, Networking and Communications (CNC19) at the International Conference on Computing, Networking and Communications (ICNC 2019), Honolulu, Hawaii, Feb. 18-21, 2019, 7 pp., <http://www.cse.wustl.edu/~jain/papers/hypervin.htm>

List of Acronyms

- ❑ AI Artificial Intelligence
- ❑ DNS Domain Name Service
- ❑ IEEE Institution of Electrical and Electronics Engineers
- ❑ IoT Internet of Things
- ❑ IP Internet Protocol
- ❑ PKI Public Key Infrastructure
- ❑ SSL Secure Socket Layer

Scan This to Download These Slides



THANK
YOU



Raj Jain

rajjain.com

http://www.cse.wustl.edu/~jain/talks/pbc_iics.htm